Práctica 7.2 Creación de una VPC en AWS Learner Lab

miércoles, 26 de febrero de 2025 16:41

Escenario

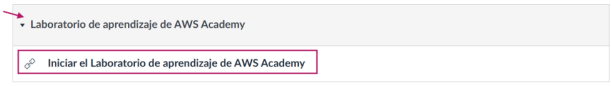
Se requiere la creación de una **VPC personalizada** con el siguiente esquema de red:

- **Rango de red de la VPC:** 10.20.0.0/16
- **Número total de subredes:** 6
  - **2 subredes públicas** (una en cada zona de disponibilidad)
  - **4 subredes privadas** (dos a dos en una misma zona de disponibilidad)
- Configurar y probar el acceso a Internet para las subredes públicas mediante un **Internet Gateway**.
- Configurar y probar la conectividad a Internet para al menos dos subredes privadas a través de un **NAT Gateway.**

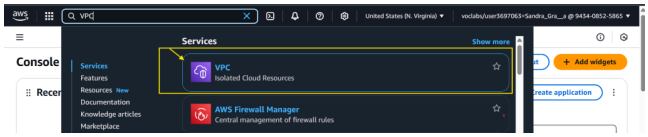
Pasos/enunciados

1. Dibuja un **esquema** de la VPC del problema descrito.

2. Inicia sesión en el aula virtual de AWS **Academy Learner Lab** y accede al apartado Lanzamiento del Laboratorio para el alumnado de AWS Academy.

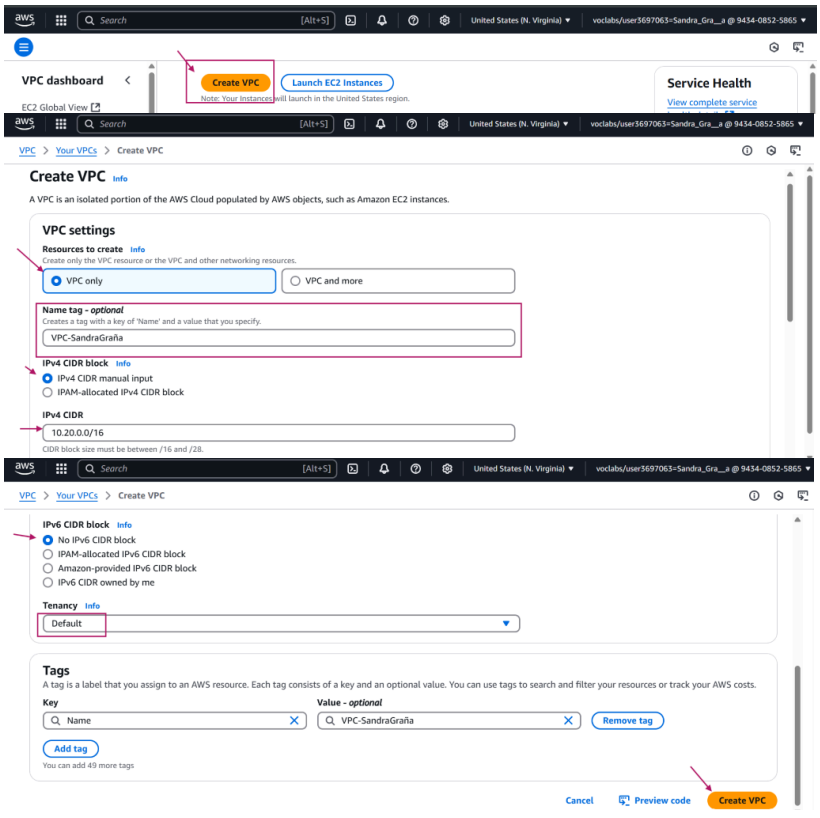


3. Accede al servicio de **VPC**.



4. Crea una **nueva VPC** con los siguientes valores:

- **Nombre:** VPC-NombreEstudiante
- **Rango de CIDR:** 10.20.0.0/16
- **Sin bloque IPv6**
- **Tenencia:** Predeterminado



5. Crea las 6 **subredes** indicadas en este apartado y la **tabla** siguiente:

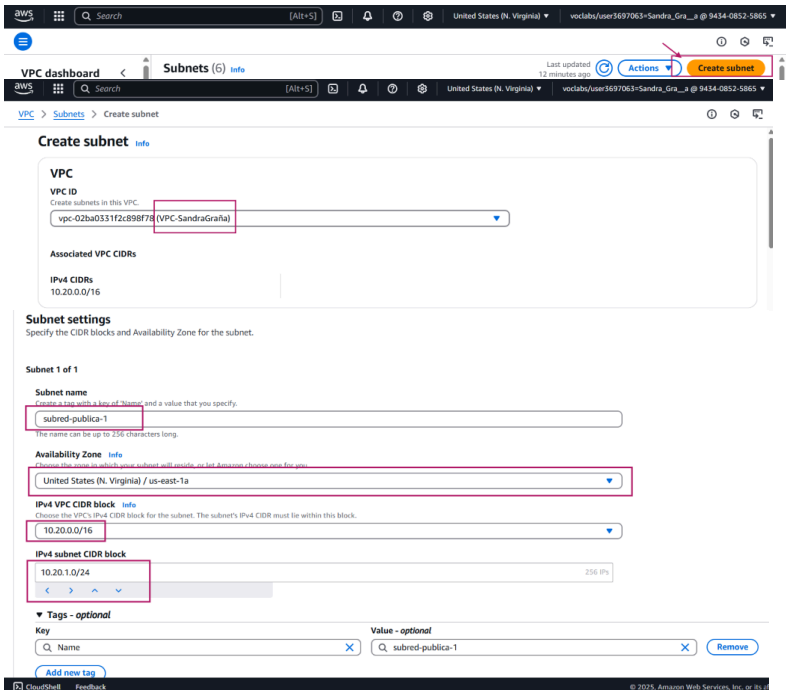
- Crear **2 subredes públicas** llamadas *subred-publica-1* y *subred-publica-2* distribuyéndolas en diferentes zonas de disponibilidad (por ejemplo, *us-east-1a* y *us-east-1b*).
- Crear **4 subredes privadas**, llamadas *subred-privada-[1-4]* distribuyéndolas dos a dos en dos zonas de disponibilidad diferentes.
- Deberás de dividir la red en segmentos más pequeños que utilicen su propia máscara de subred para un total de **251** posibles instancias cada una y especificarlo en el **Rango CIDR**.

Nombre	Tipo	Zona disponibilidad	Rango CIDR
subred-publica-1	Pública	us-east-1a	10.20.1.0/24
subred-publica-2	Pública	us-east-1b	10.20.2.0/24
subred-privada-1	Privada	us-east-1a	10.20.3.0/24
subred-privada-2	Privada	us-east-1a	10.20.4.0/24
subred-privada-3	Privada	us-east-1b	10.20.5.0/24
subred-privada-4	Privada	us-east-1b	10.20.6.0/24

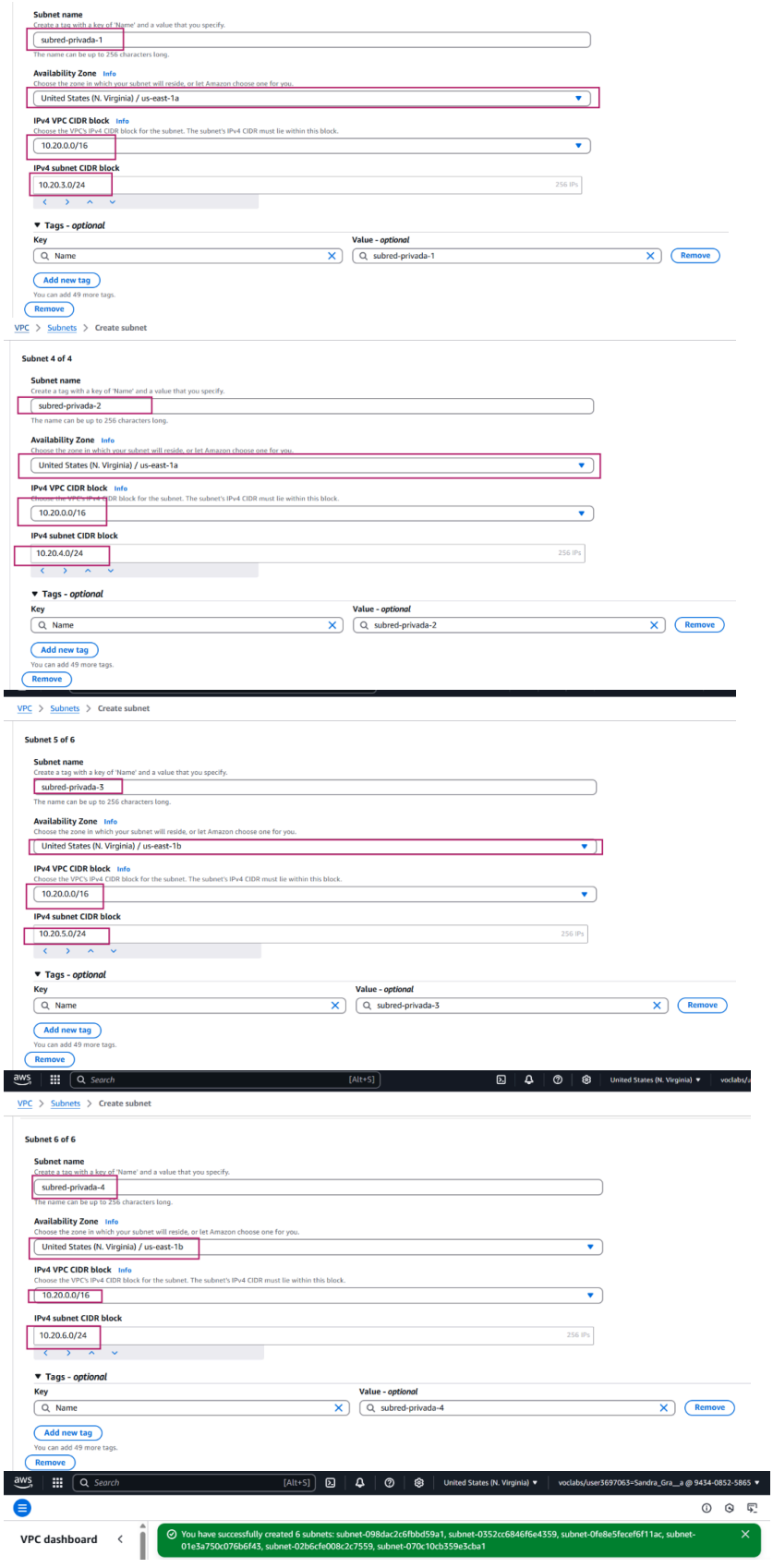
Utilizamos una máscara de subred **/24** (que permite hasta 254 hosts, restando direcciones reservadas para la red y el gateway).

Pasos para crear:

1. Create Subnet
2. Elegir VPC
3. Crear cada subred con:
   i. Su nombre
   ii. Su zona
   iii. Su CIDR Rango
4. Add new Subnet

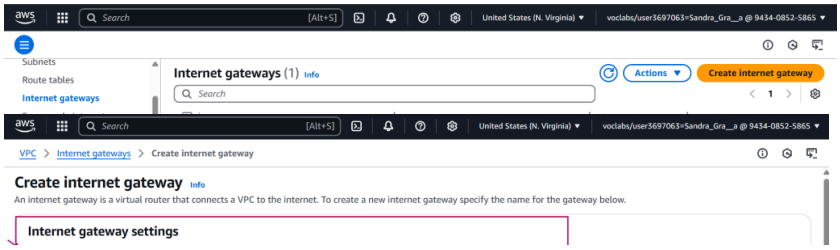


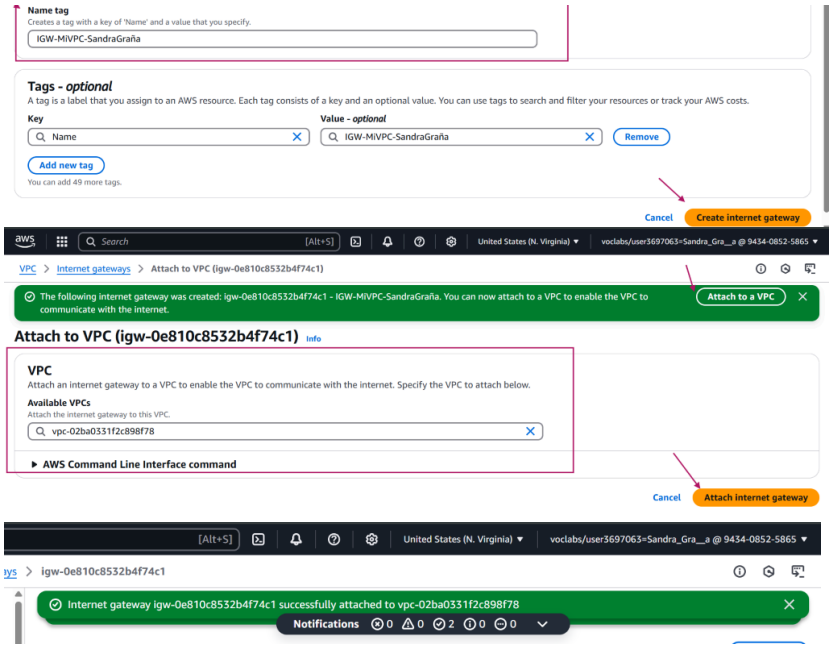
* Cambie el nombre (Me equivoque le he puesto privada y es publica)



6. Crear y configurar un **Internet Gateway (IGW)**
   a. Crea un **Internet Gateway** en el puertas de enlace de Internet llamado IGW-MiVPC-NombreEstudiante

   b. Una vez que lo has creado adjúntalo a tu VPC desde el listado de Gateways.

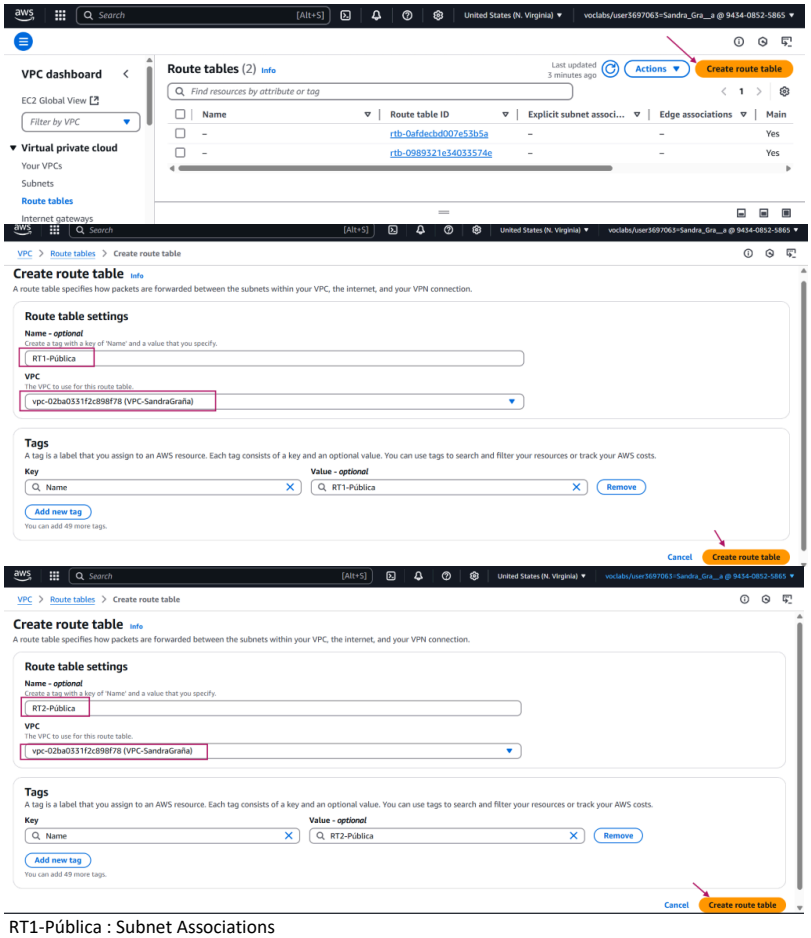




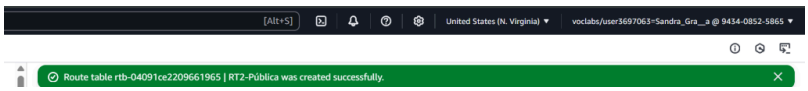
7. Crea y asociar **tablas de enrutamiento** para las **subredes públicas.**
   a. Crear dos nuevas tablas de rutas para cada subred pública, llamadas RT1-Pública y RT2-Pública.
   b. En el apartado **asociaciones de subred** asignarlas a sus correspondientes subredes públicas.
   c. En cada tabla creada, ve a **agregar ruta** y añade lo siguiente:
      - **Destino:** 0.0.0.0/0
      - **Target:** Puerta de enlace de Internet (el IGW creado en el paso anterior).

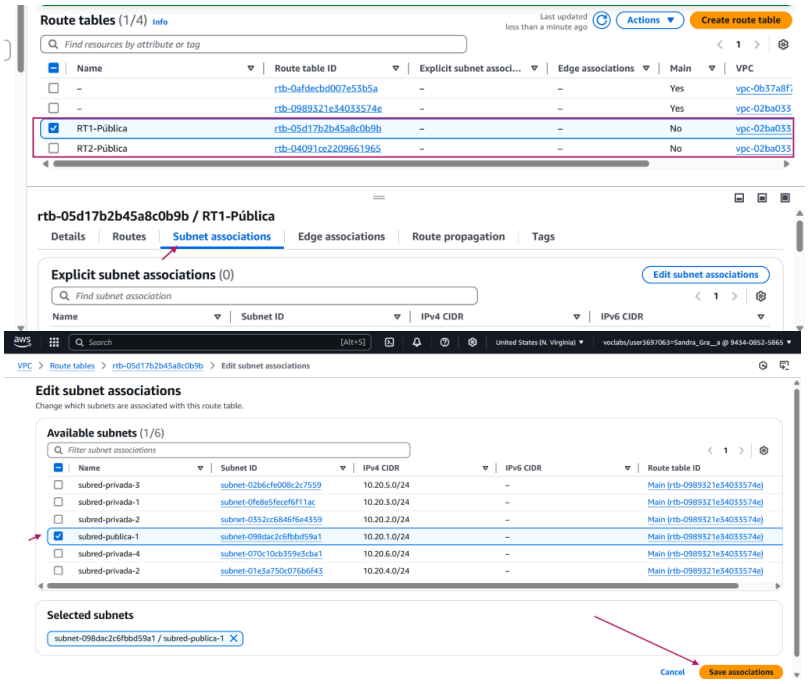
Pasos:

1. Create Route Table:
   i. Nombre
   ii. VPC
2. Seleccionar Tablas e ir a Route Associations

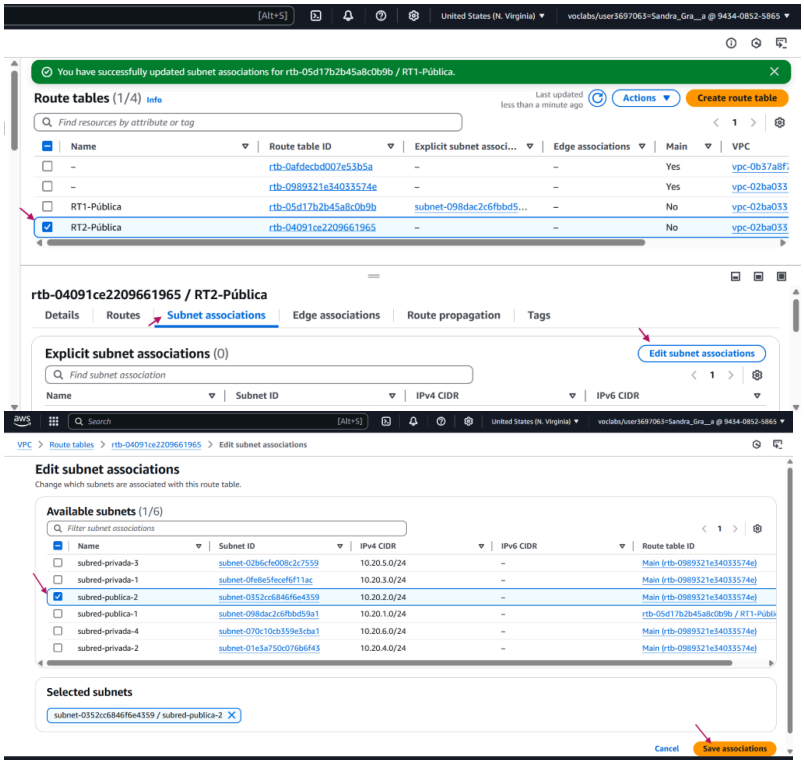


RT1-Pública : Subnet Associations





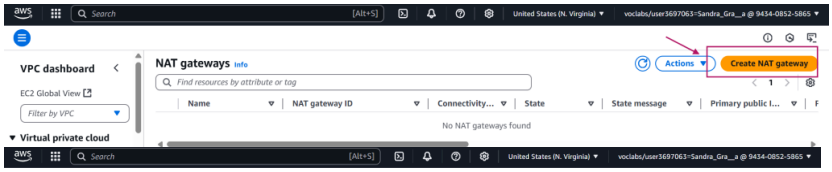
RT2-Pública : Subnet Associations

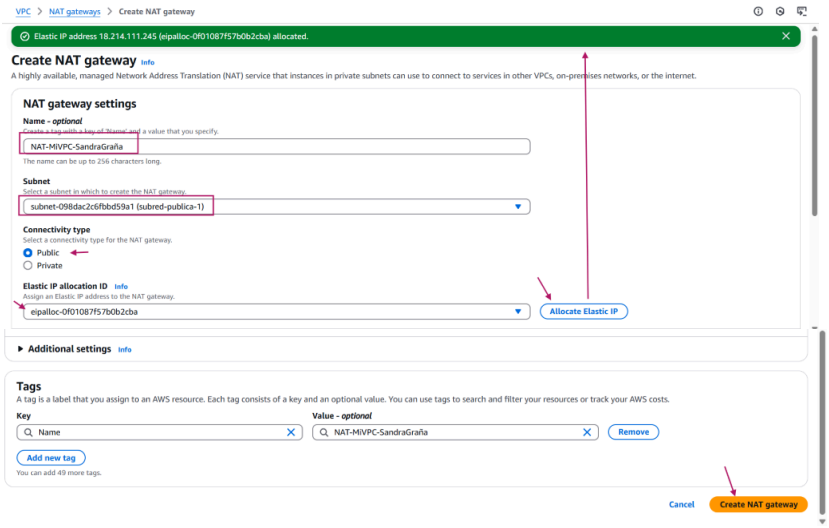


8. Crear y configurar un **NAT Gateway.**
   a. Crea un **NAT Gateway** llamado NAT-MiVPC-NombreEstudiante
   b. En el apartado subred indica una subred pública dentro de tu VPC (Nota importante: los NAT Gateways van configurados a una red pública para dar salida de la subred a Internet)
   c. En el apartado **dirección IP elástica**, crear una **nueva.**
   Al hacer clic en crear, en NAT tardará un momento en crearse (aparecerá en estado *pending*)

Pasos:

1. Create NAT Gateway:
   i. Nombre
   ii. Asociar Subred Publica
   iii. Indicar tipo
   iv. dirección IP elástica (Allocate)

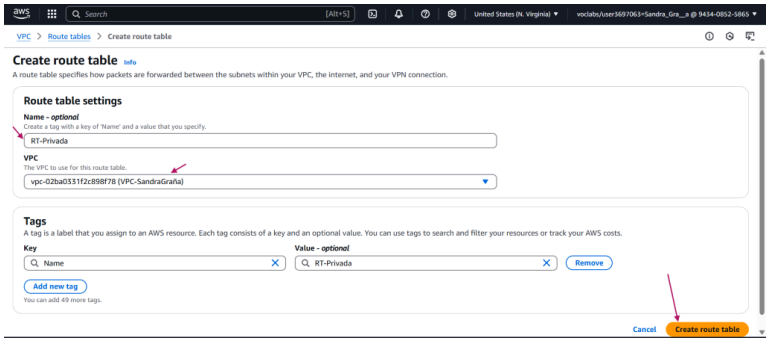




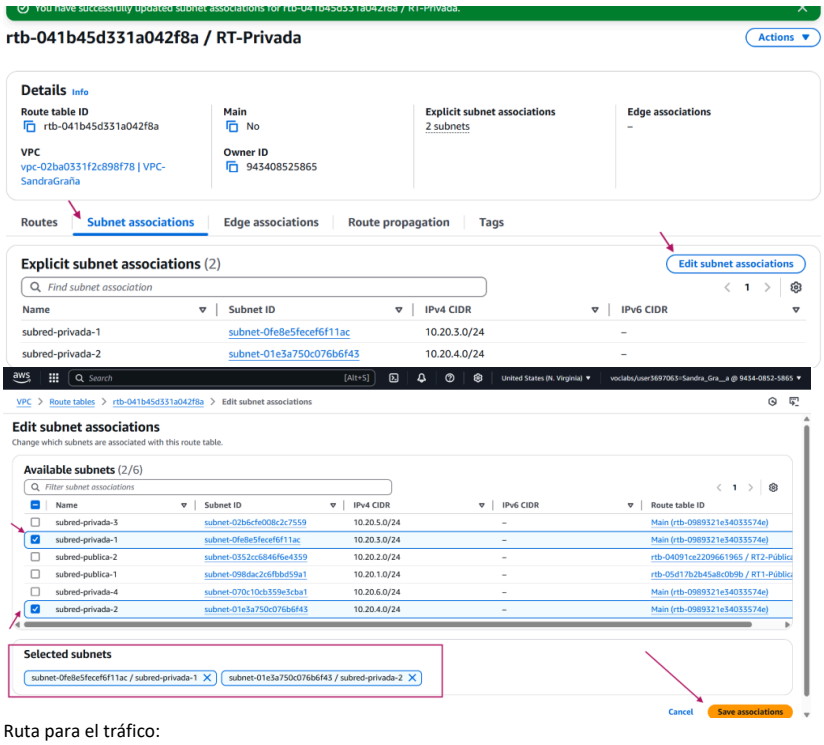
9. Asociar <u>al menos dos</u> **subredes privadas** al **NAT Gateway**
   - **Modificar las tablas de rutas de las subredes privadas:**
     a. Dirígete al apartado **tablas de enrutamiento** del panel lateral izquierdo.
     b. Crea una nueva tabla de rutas para las subredes privadas llamada RT-Privada
     c. En **asociaciones de subredes**, asigna las siguientes subredes privadas a la tabla:
        - subred-privada-1
        - subred-privada-2
   - **Configurar la ruta para el tráfico de Internet:**
     a. En la tabla de rutas creada, accede a la pestaña **rutas** y haz clic en editar rutas.
     b. Añade la tabla creada, agrega la siguiente **regla**:

        Destino: 0.0.0.0/0
        Target: Puerta de enlace NAT (el NAT Gateway creado en el paso anterior).

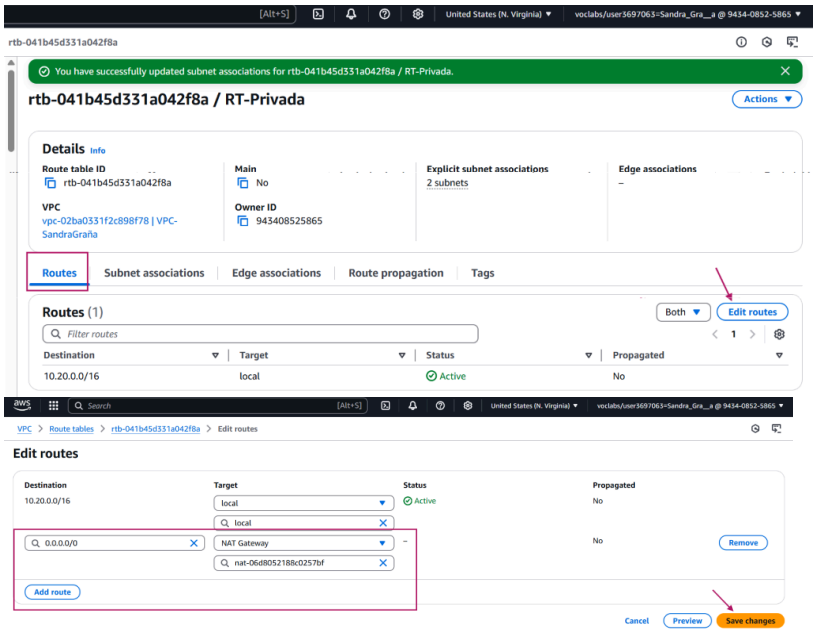
Creación de tabla enrutamiento privada: RT-Privada



Asociación de Subredes:



Ruta para el tráfico:

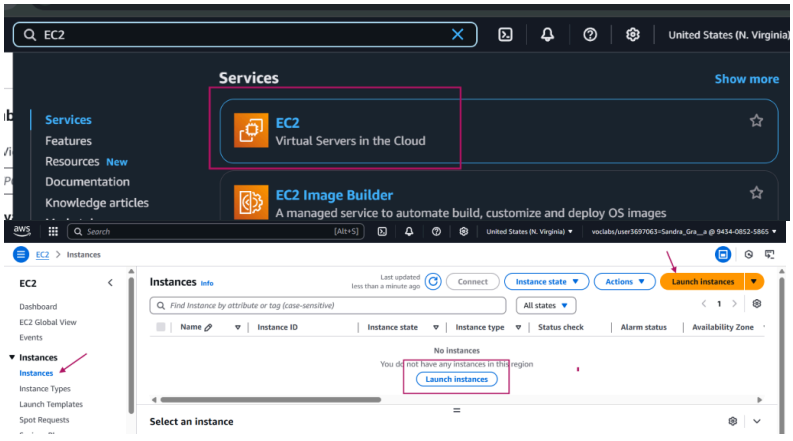


10. Revisa y prueba la **conectividad** con **dos instancias de prueba**.

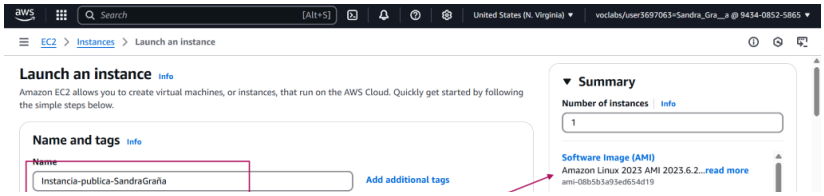
- Lanza una instancia en una **subred pública** para verificar la conectividad a Internet.
    a. Crea una instancia en **EC2** de Amazon Linux por ejemplo y llámala Instancia-publica-NombreEstudiante
    b. No te olvides seleccionar un par de claves de inicio de sesión.
    c. En el apartado de **configuraciones de red**:
        - Selecciona la VPC que creaste anteriormente.
        - Selecciona una subred pública de las que creaste.
        - Habilita asignar automáticamente la IP pública.
        - En **configuración de red avanzada** escribe en IP principal una de la del rango de la subred pública que hayas seleccionado.
    d. Conéctate a la instancia y desde la consola y haz ping a www.google.com y si funciona es que todo está bien configurado.

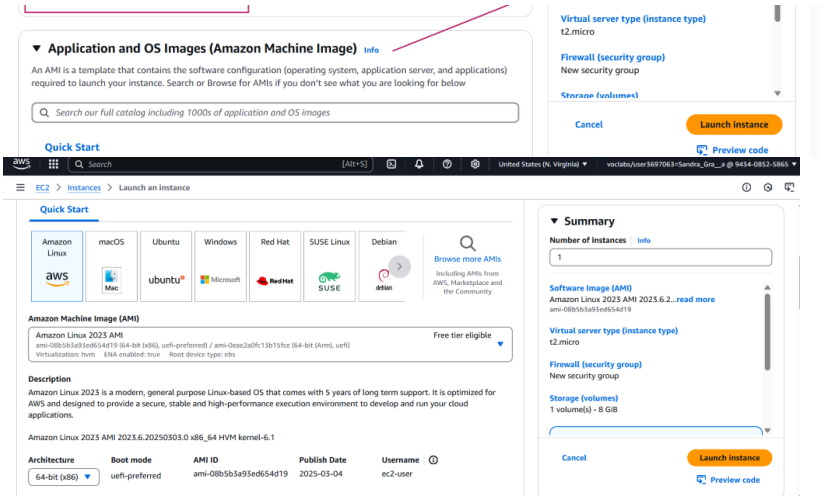
- Lanza una instancia en una **subred privada** para verificar que pueda salir a Internet a través del NAT Gateway.
    a. Crea una nueva instancia siguiendo los pasos anteriores y llámala Instancia-privada-NombreEstudiante
    b. En el apartado de **configuraciones de red**:
        - Selecciona ahora una **subred privada** con acceso al NAT Gateway de las que creaste.
        - Desactiva la opción de asignar automáticamente una IP pública, ya que la instancia estará en una subred privada.
        - En **configuración de red avanzada** escribe en IP principal una de la del rango de la subred privada que hayas seleccionado.
    c. Conéctate a la instancia y verifica hacer ping a una dirección para comprobar si se puede acceder a la red.

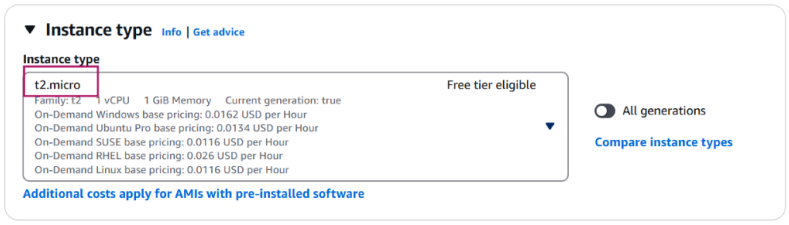
Para ambas instancias tienes que entrar en EC2:

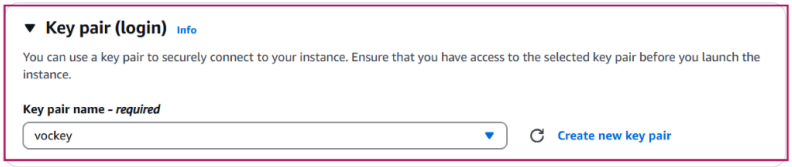


INSTANCIA PARA SUBRED PUBLICA:

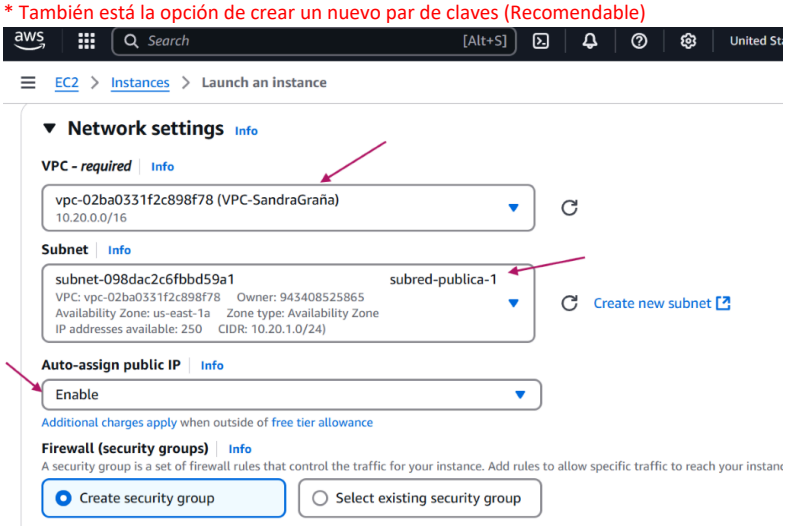


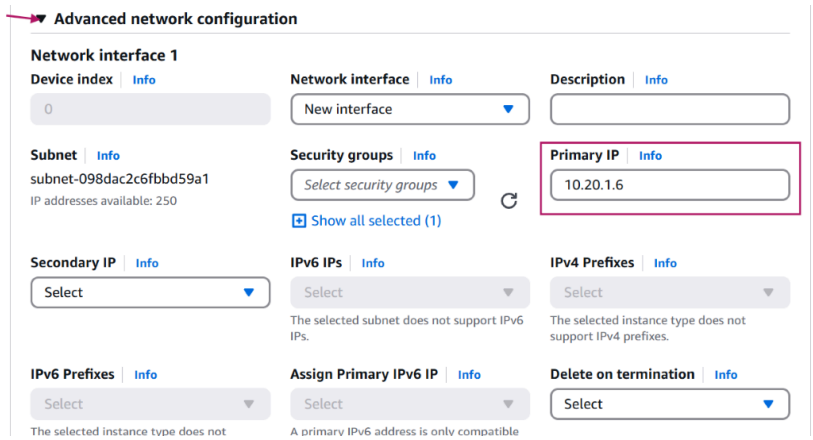






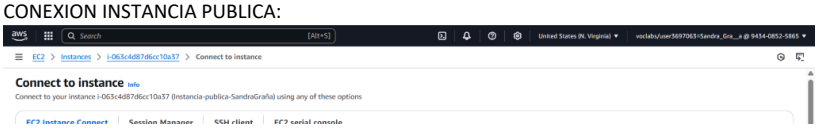
* También está la opción de crear un nuevo par de claves (Recomendable)

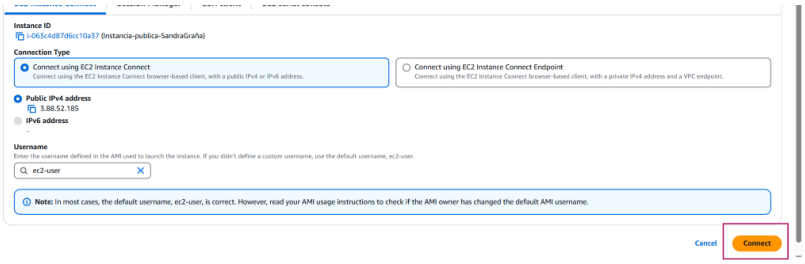


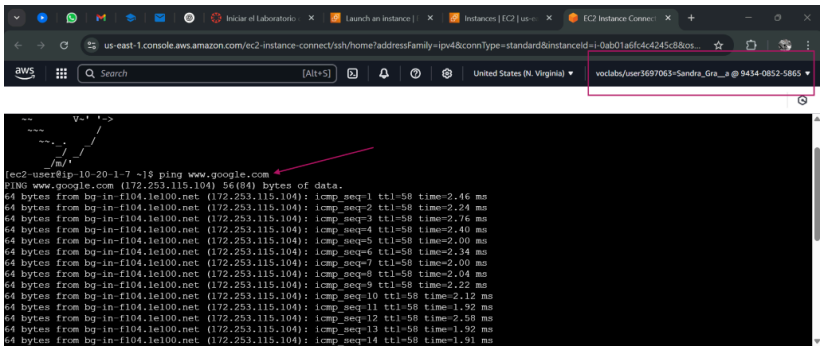


* Al poner la IP ten en cuenta de que las 5 primeras están reservadas. Así que usa .6 o .7

CONEXION INSTANCIA PUBLICA:

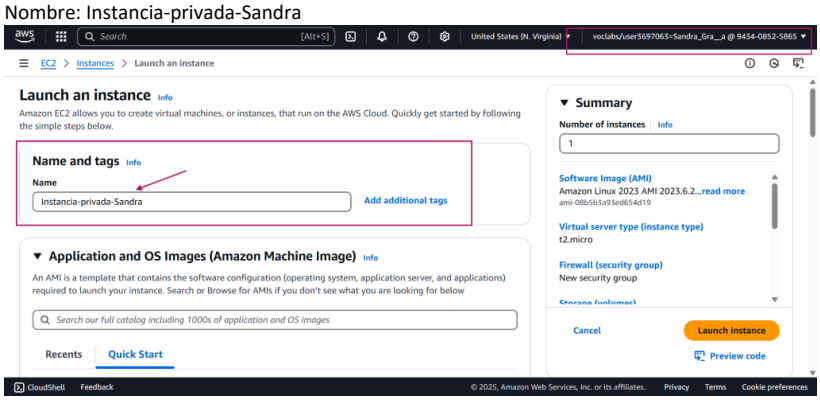




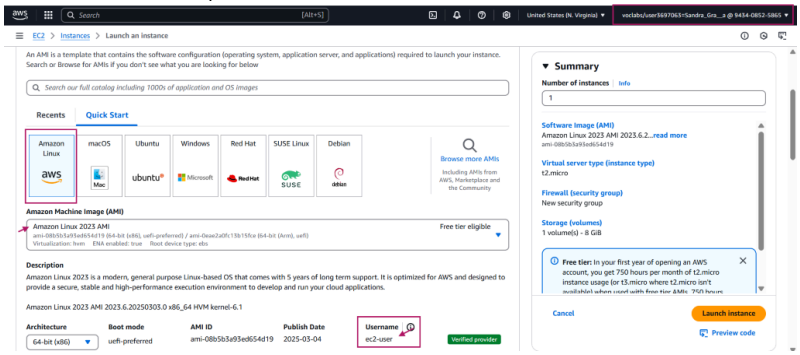


INSTANCIA PARA SUBRED PRIVADA:

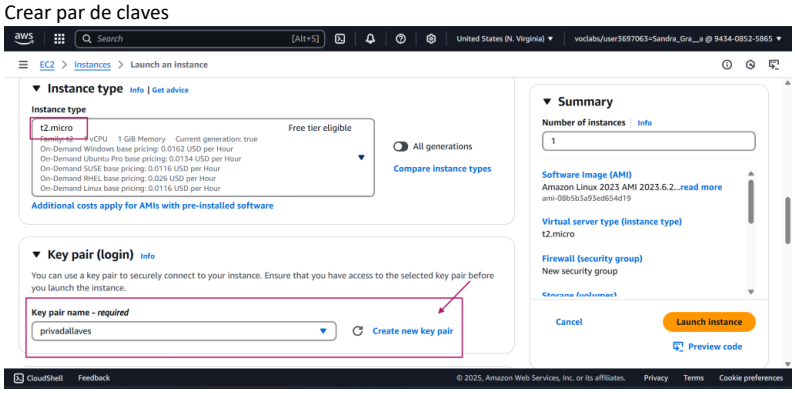
Nombre: Instancia-privada-Sandra



AMI: Amazon Linux (Porque esta EC2 Instance Connect habilitado por defecto)
Usaremos el username para conectarnos: e2-user



Tipo de Instancia: Defecto
Crear par de claves



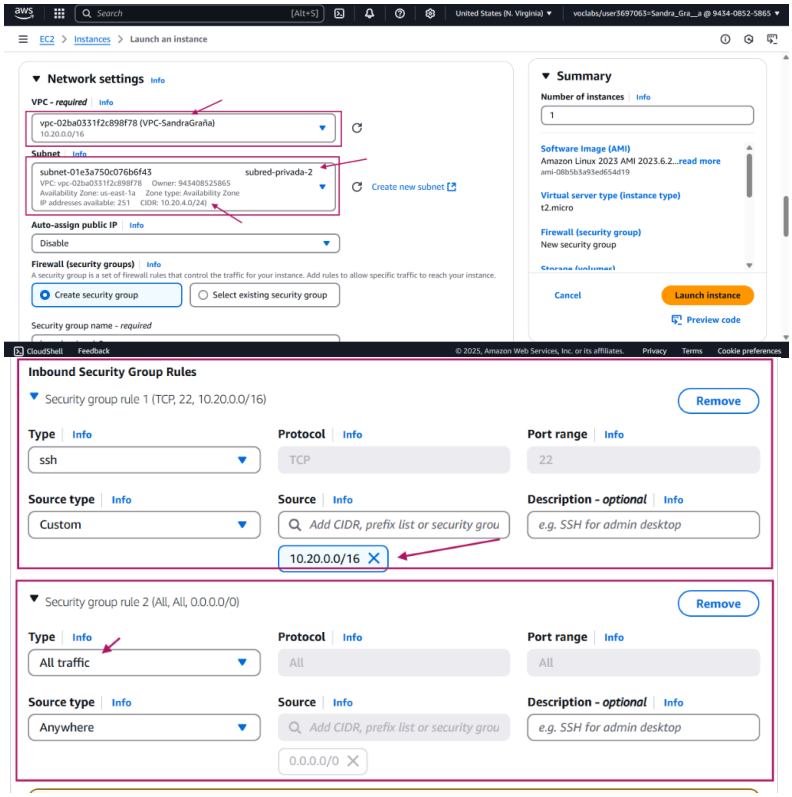
Configuración de red:

- VPC: Selecciona la VPC donde configuraste el NAT Gateway
- Subred: Selecciona una subred privada con acceso al NAT Gateway

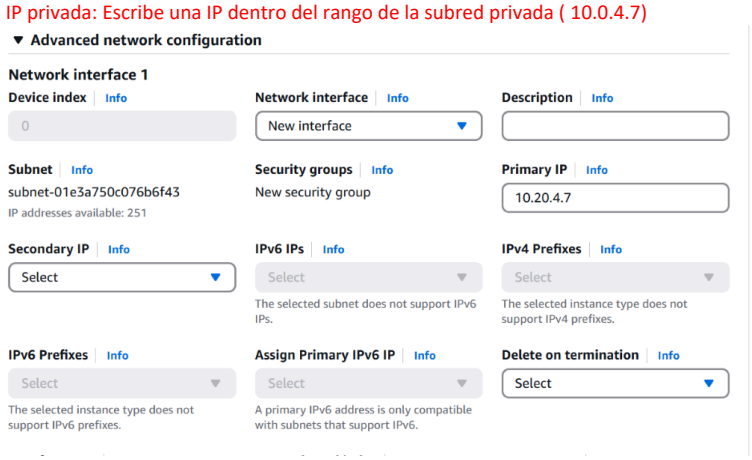
- Asignar IP pública automáticamente: Desactivado

Grupo de seguridad:

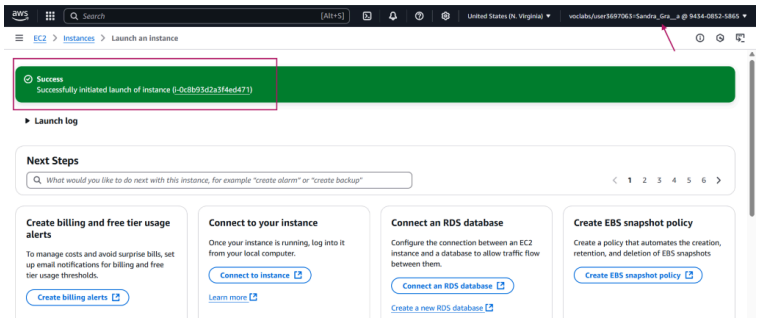
- Permitir conexión SSH (puerto 22) desde la subred pública o desde un VPC Endpoint
- Permitir tráfico de salida a Internet (0.0.0.0/0)



* IP privada: Escribe una IP dentro del rango de la subred privada (10.0.4.7)

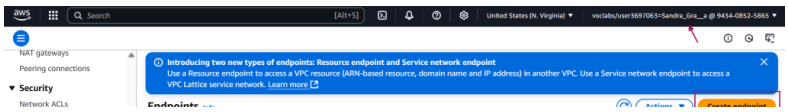


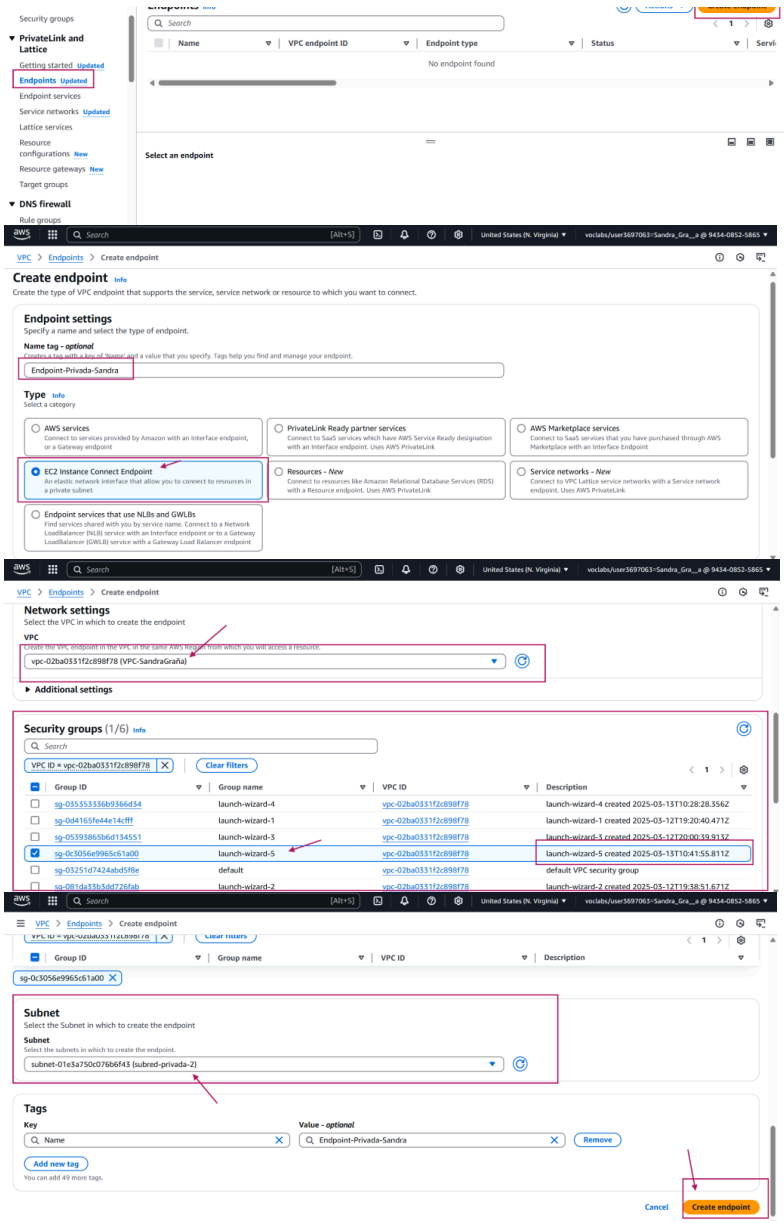
CONEXION INSTANCIA PRIVADA:



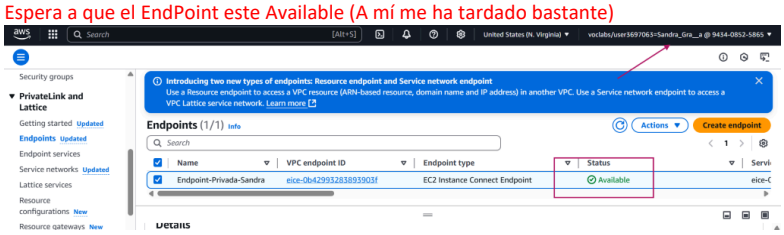
Ahora hay que crear un ENDPOINT en VPC:

- Nombre (Instancia-Privada-Sandra)
- Elegir el tipo con interfaz para EC2 instance connect (Que es de donde nos conectaremos)
- Elegir la VPC donde está la subred privada
- Elegir el grupo de seguridad que has usado en la instancia (En mi caso es la 5)
- Elegir la subred privada que está en la instancia

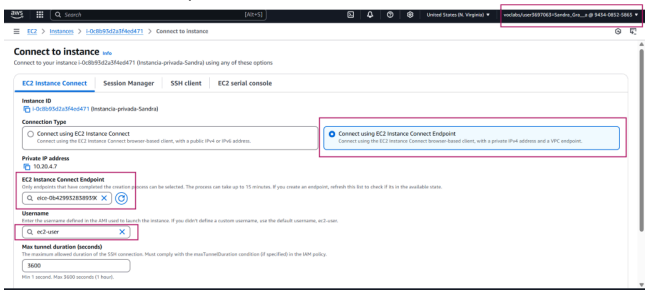




Espera a que el EndPoint este Available (A mí me ha tardado bastante)



Conéctate con EC2 Endpoint Connect:



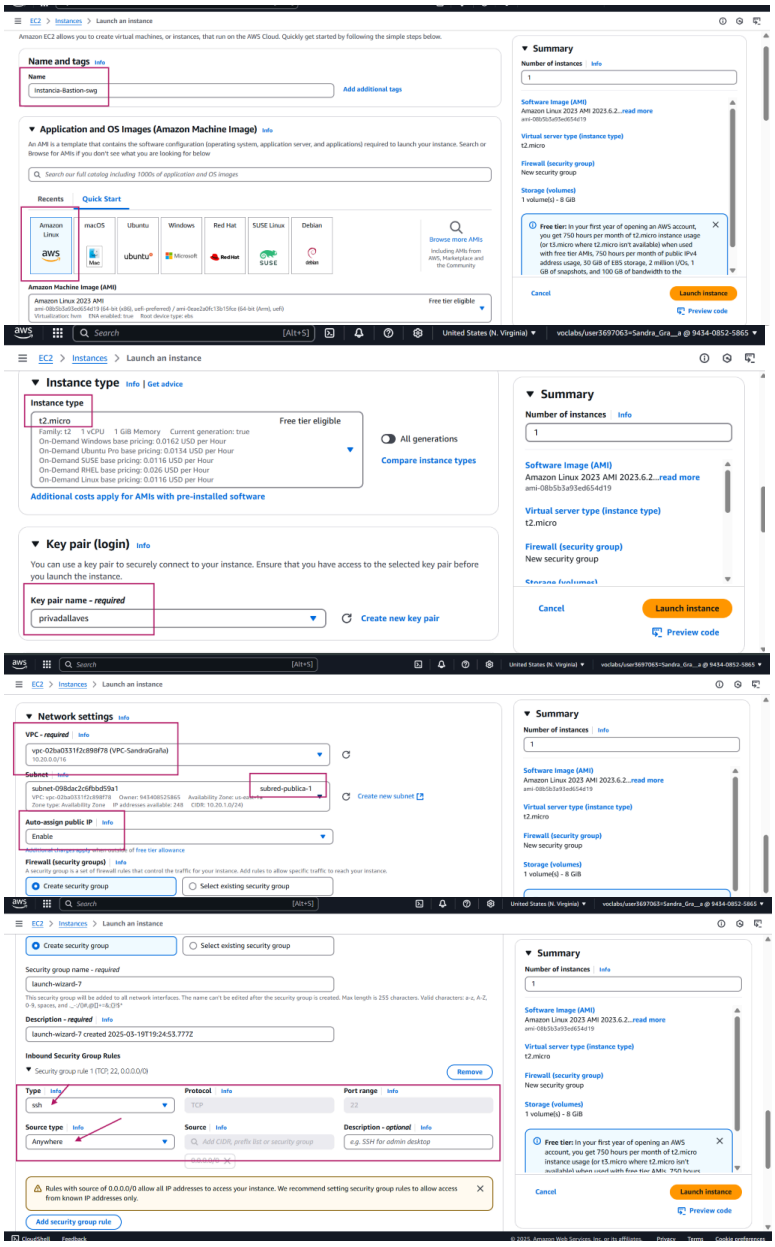
CONEXION A INSTANCIA PRIVADA CON SSH Y BASTION:

Crear instancia Bastion, necesita:

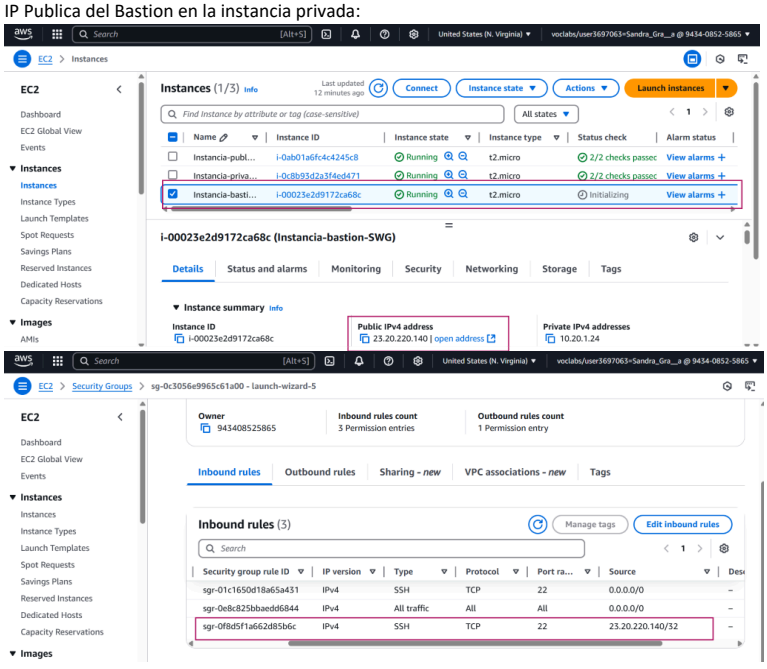
- VPC de la instancia privada
- Mismo par de claves
- Dirección IP publica auto
- SSH

Después en la instancia privada:

- Debes de poner en el grupo de seguridad SSH con origen: IP del bastion host.



IP Publica del Bastion en la instancia privada:



CONEXION CON SSH EN TERMINAL CMD:

- Debes estar en la carpeta donde está el par de llaves, en mi caso es en Downloads
- Copia el par de llaves en la instancia bastion:
  - scp -i "privadallaves.pem" privadallaves.pem ec2-user@23.20.220.140:~
- Entra en la instancia bastion con ssh:

    - ssh -i "privadallaves.pem" ec2-user@23.20.220.140
- Aquí dale permisos (te lo pide aws): chmod 400 para esconderlo
- Conectate con SSH a la instancia privada:
    - Puedes hacer ping a su ip privada para asegurarte de que lo vea.
    - ssh -i "privadallaves.pem" ec2-user@10.20.4.7